



SPYWOLF

Security Audit Report



Completed on
September 23, 2022

MADE IN USA 

@SPYWOLFNETWORK



@SPYWOLFNETWORK



SPYWOLF.CO





OVERVIEW

This audit has been prepared for **SenCoin** to review the main aspects of the project to help investors make an informative decision during their research process.

You will find a summarized review of the following key points:

- ✓ Contract's source code
- ✓ Owners' wallets
- ✓ Tokenomics
- ✓ Team transparency and goals
- ✓ Website's age, code, security and UX
- ✓ Whitepaper and roadmap
- ✓ Social media & online presence

“

The results of this audit are purely based on the team's evaluation and does not guarantee nor reflect the projects outcome and goal

- SPYWOLF Team -

”





TABLE OF CONTENTS

Project Description	01
Contract Information	02
Current Stats	03-04
Featured Wallets	05
Vulnerability Check	06
Threat Levels	07
Found Threats	08-A/08-D
Good Practices	09
Tokenomics	10
Team Information	11
Website Analysis	12
Social Media & Online Presence	13
About SPYWOLF	14
Disclaimer	15



SenCoin



PROJECT DESCRIPTION

According to their whitepaper:

SenCoin's objective is to be the leader in the crypto currency market in Senegal. SenCoin token will be used mainly as a current digital currency to pay for goods and services through a peer to peer application. Most of the funds from sales will be injected into education (creation and renovation of schools, allocation of social grants...) and training, in the promotion and support of African business development.

Release Date: Presale starts on Sep, 2021

Category: Finance



CONTRACT INFO

Token Name
SenCoin TOKEN

Symbol
XSN

Contract Address
0x186220e9b319b003ad0b63532D9AA47E1465d117

Network
Binance Smart Chain

Language
Solidity

Deployment Date
Sep 21, 2022

Verified?
Yes

Total Supply
80,000,000

Status
Not launched

TAXES

Buy Tax
5%

Sell Tax
5%

*Taxes can be changed in future



Our Contract Review Process

The contract review process pays special attention to the following:

- ✓ Testing the smart contracts against both common and uncommon vulnerabilities
- ✓ Assessing the codebase to ensure compliance with current best practices and industry standards.
- ✓ Ensuring contract logic meets the specifications and intentions of the client.
- ✓ Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- ✓ Thorough line-by-line manual review of the entire codebase by industry experts.

Blockchain security tools used:

- OpenZeppelin
- Mythril
- Solidity Compiler
- Hardhat



CURRENT STATS

(As of Sep 23, 2022)



Liquidity

Not added yet



Burn

No burnt tokens

Status:
Not Launched!

MaxTxAmount
800,000

DEX:
PancakeSwap

LP Address(es)

Liquidity not added yet



TOKEN TRANSFERS STATS

Transfer Count	1
Uniq Senders	1
Uniq Receivers	1
Total Amount	80000000 XSN
Median Transfer Amount	80000000 XSN
Average Transfer Amount	80000000 XSN
First transfer date	2022-09-21
Last transfer date	2022-09-21
Days token transferred	1

SMART CONTRACT STATS

Calls Count	3
External calls	3
Internal calls	0
Transactions count	3
Uniq Callers	2
Days contract called	2
Last transaction time	2022-09-22 08:56:31 UTC
Created	2022-09-21 12:26:53 UTC
Create TX	0xe0187c6d080b010b33d058663beb40fc7a e30449258a16c61d4fbe2c7e82d2fd
Creator	0x9e68d3379218627524a93231c625a780cf2 0caa4



FEATURED WALLETS

Owner address	0x9e68d3379218627524a93231c625a780cf20caa4
LP address	Liquidity not added yet

TOP 3 UNLOCKED WALLETS

1



Same as owner

*Same as owner



VULNERABILITY CHECK

Design Logic	Passed
Compiler warnings.	Passed
Private user data leaks	Passed
Timestamp dependence	Passed
Integer overflow and underflow	Passed
Race conditions and reentrancy. Cross-function race conditions	Passed
Possible delays in data delivery	Passed
Oracle calls	Passed
Front running	Passed
DoS with Revert	Passed
DoS with block gas limit	Passed
Methods execution permissions	Passed
Economy model	Passed
Impact of the exchange rate on the logic	Passed
Malicious Event log	Passed
Scoping and declarations	Passed
Uninitialized storage pointers	Passed
Arithmetic accuracy	Passed
Cross-function race conditions	Passed
Safe Zeppelin module	Passed
Fallback function security	Passed



THREAT LEVELS

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time. We categorize these vulnerabilities by the following levels:

High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Low Risk

Issues on this level are minor details and warning that can remain unfixed.

Informational

Information level is to offer suggestions for improvement of efficacy or security for features with a risk free factor.



FOUND THREATS

⚠ High Risk

Owner can blacklist address from trading, making it impossible to sell.

```
function bulkBlacklist(address[] memory accounts) external onlyOwner returns (bool) {  
    for(uint i=0; i < accounts.length; i++){  
        _isBlacklisted[accounts[i]] = true;  
    }  
    return true;  
}
```

Potential large array looping.

```
function multiTransfer(address[] memory recipients, uint256[] memory amount) public override returns (bool) {  
    for(uint i=0; i < recipients.length; i++){  
        _transfer(_msgSender(), recipients[i], amount[i]);  
    }  
    return true;  
}
```

- Recommendation:
 - Good practice while looping through dynamic arrays of unknown size to avoid denial of service (DOS) is to put limitation of either array iterations and/or gas limit, less than the current block gas limit. Current gas block limit can be found at <https://bscscan.com/blocks>
Further reference: <https://swcregistry.io/docs/SWC-128>



FOUND THREATS

⚠ High Risk

Owner can set buy/sell/transfer fees up to 100%.

```
function setFeesTransfer(uint taxFee, uint liquidityFee) external onlyOwner {
    _taxFee = taxFee;
    _liquidityFee = liquidityFee;
}

function setBuyFees(uint taxFee, uint liquidityFee) external onlyOwner {
    _taxFeeBuy = taxFee;
    _liquidityFeeBuy = liquidityFee;
}

function setSellFees(uint taxFee, uint liquidityFee) external onlyOwner {
    _taxFeeSell = taxFee;
    _liquidityFeeSell = liquidityFee;
}
```

- Recommendation:
 - Considered as good tax deduction practice is buy and sell fees combined not to exceed 25%.



FOUND THREATS

⚠ High Risk

If auto swap is on and `_minTokenBalance` is set to 0, selling will fail.

If the result of the following *variables is above 10000, selling will fail.

* `_percentageOfLiquidityForTeam` + * `_percentageOfLiquidityForMarketing`

```
function setMinTokenBalance(uint256 minTokenBalance) external onlyOwner {
    _minTokenBalance = minTokenBalance;
}

function setLiquidityPercentages(uint256 teamFee, uint256 marketingFee) external onlyOwner {
    _percentageOfLiquidityForTeam = teamFee;
    _percentageOfLiquidityForMarketing = marketingFee;
}

function _transfer(
    address from,
    address to,
    uint256 amount
) private {
    .....

    if (
        isOverMinTokenBalance &&
        !inSwapAndLiquify &&
        !_isExcludedFromAutoLiquidity[from] &&
        swapAndLiquifyEnabled
    ) {
        contractTokenBalance = _minTokenBalance;
        swapAndLiquify(contractTokenBalance);
    }
    .....
}

function swapAndLiquify(uint256 contractTokenBalance) private lockTheSwap {
    .....
    uint256 newBalance = address(this).balance - initialBalance;
    uint256 bnbForTeam = newBalance / 10000 * _percentageOfLiquidityForTeam;
    uint256 bnbForMarketing = newBalance / 10000 * _percentageOfLiquidityForMarketing;
    uint256 bnbForLiquidity = newBalance - bnbForTeam - bnbForMarketing;
    .....
}
```

- Recommendation:
 - Limitations must be put for `minTokenBalance` variable to ensure it is always above 0.
 - Limitations for the sum of `_percentageOfLiquidityForTeam` + `_percentageOfLiquidityForMarketing` variables must be included to ensure it is always 10000.



Informational

Owner can exclude address from fees, transaction and delay limit.

```
function setExcludedFromFee(address account, bool e) external onlyOwner {
    _isExcludedFromFee[account] = e;
}

function setExcludedFromMaxTx(address account, bool e) external onlyOwner {
    _isExcludedFromMaxTx[account] = e;
}

function setExcludedFromBuy(address account, bool e) external onlyOwner {
    _isExcludedFromBuy[account] = e;
}
```

Owner can set delay between trades up to 255 seconds.

```
function cooldownEnabled(bool _status, uint8 _interval) public onlyOwner {
    opCooldownEnabled = _status;
    cooldownTimerInterval = _interval;
}
```



RECOMMENDATIONS FOR

GOOD PRACTICES

1

Consider fundamental tradeoffs

2

Be attentive to blockchain properties

3

Ensure careful rollouts

4

Keep contracts simple

5

Stay up to date and track development

SenCoin

GOOD PRACTICES FOUND

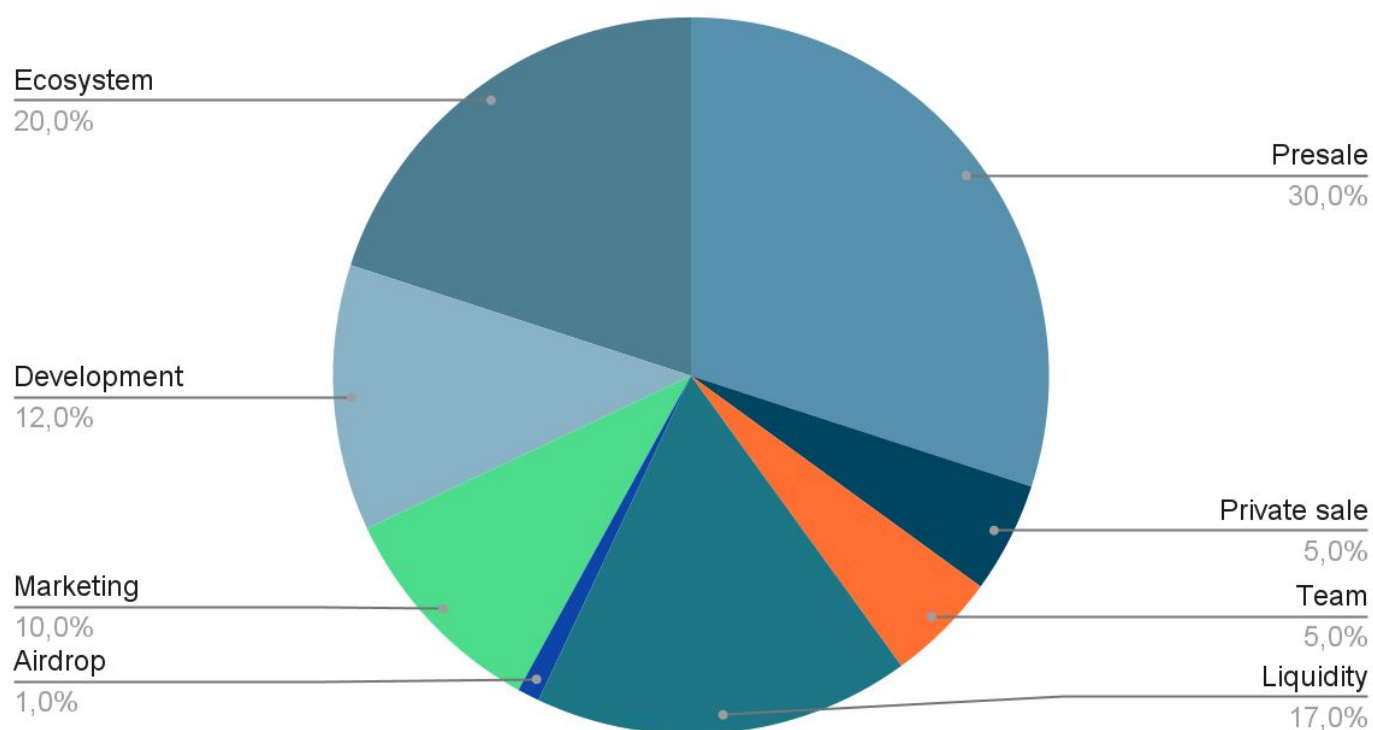
- ✓ The owner cannot mint new tokens after deployment
- ✓ The owner cannot set a transaction limit. Fixed max transaction limit for 1% of total supply is in effect.



*The following tokenomics are based on the project's whitepaper and/or website:

- 30% - Presale
- 5% - Private sale
- 20% - Ecosystem
- 1% - Airdrop
- 5% - Team
- 12% - Development
- 10% - Marketing
- 17% - Liquidity

Tokens distribution



TOKENOMICS



THE TEAM

✓ The team at SenCoin is publicly doxxed on their website with proven LinkedIn and Twitter profiles.



OMAR
CEO & CO-FOUNDER



OUSSEYNOU
CTO & CO-FOUNDER



MODOU
CIO & CO-FOUNDER



MADY
TEAM COM & CO-FOUNDER



SANTY
STRATEGIES & COMMUNICATION



MAMADOU
DATA ANALYSTE



MOUSTAPHA
TEAM MARKETING



OMAR
MARKETING & INNOVATIONS





WEBSITE

Website URL
<https://sencoin.net/>

Domain Registry
<https://ionos.com>

Domain Expiration
Expires on 2023-04-18

Technical SEO Test
Passed

Security Test
Passed. SSL certificate present

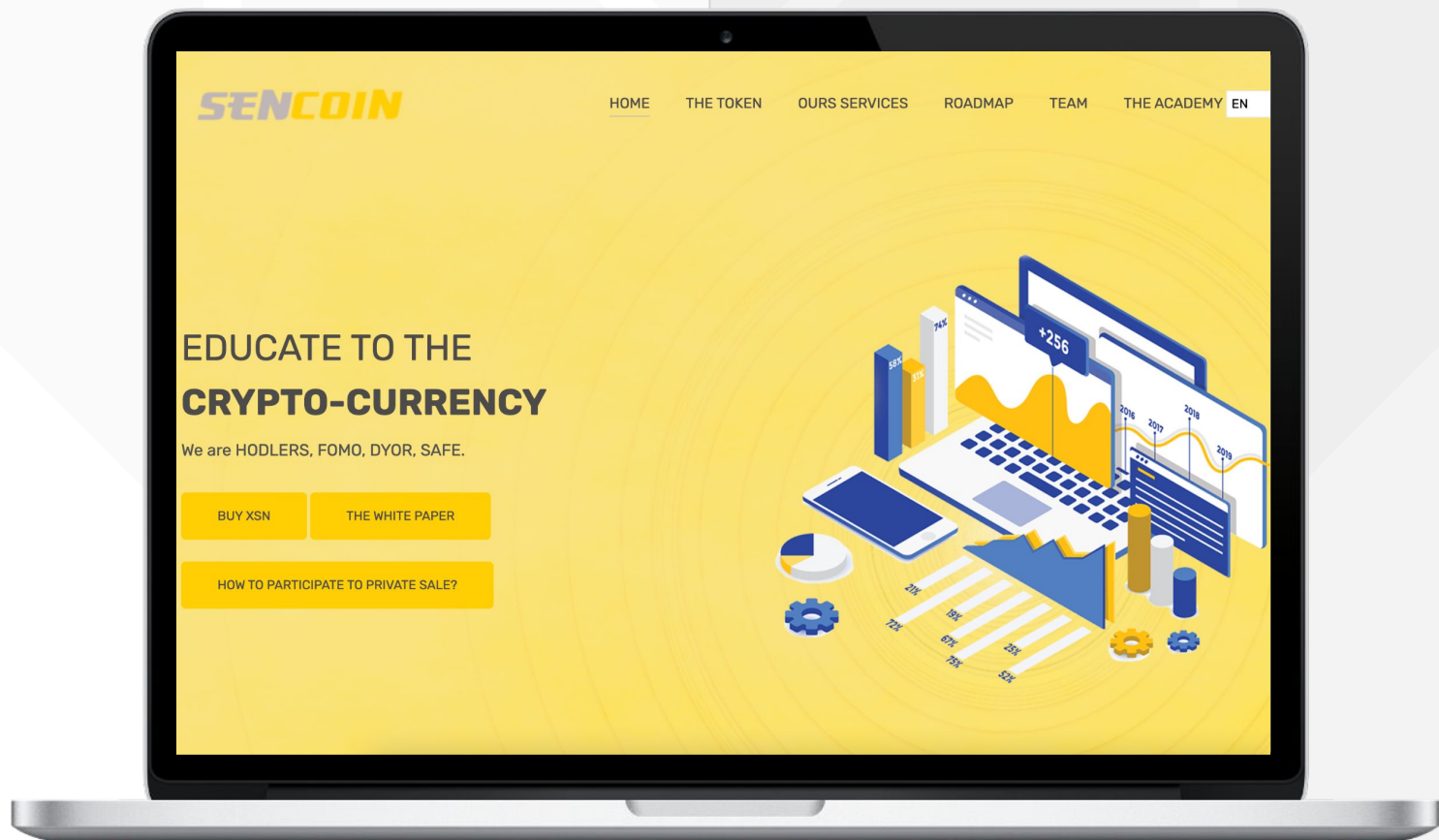
Design
Single page design,
appropriate color scheme
and graphics.

Content
The information helps new
investors understand what
the product does right away.
No grammar mistakes
found.

Whitepaper
Well written, explanatory.

Roadmap
Yes, goals set at 4 phases
with time frames.

Mobile-friendly?
Yes



sencoin.net

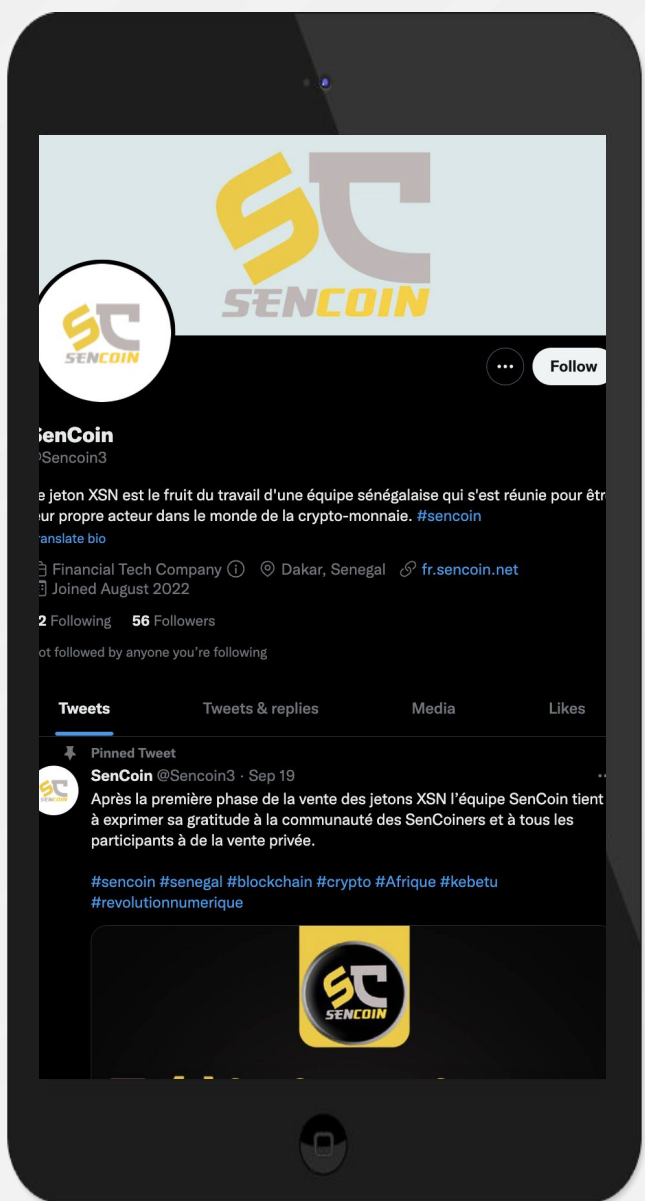


SOCIAL MEDIA

& ONLINE PRESENCE

ANALYSIS

Project's social media activity is concentrated in twitter



Twitter

@Sencoin3

- 56 followers
- Active, posts and retweets frequently



Discord

- Not available



Telegram

@sencoinen

- 14 members
- ⚠ No active members
- ⚠ No active mods



Medium

- Not available



SPYWOLF

CRYPTO SECURITY

Audits | KYCs | dApps
Contract Development

ABOUT US

We are a growing crypto security agency offering audits, KYCs and consulting services for some of the top names in the crypto industry.

- ✓ OVER 150 SUCCESSFUL CLIENTS
- ✓ MORE THAN 500 SCAMS EXPOSED
- ✓ MILLIONS SAVED IN POTENTIAL FRAUD
- ✓ PARTNERSHIPS WITH TOP LAUNCHPADS, INFLUENCERS AND CRYPTO PROJECTS
- ✓ CONSTANTLY BUILDING TOOLS TO HELP INVESTORS DO BETTER RESEARCH

To hire us, reach out to
contact@spywolf.co or
t.me/joe_SpyWolf

FIND US ONLINE



SPYWOLF.CO



SPYWOLF.NETWORK



@SPYWOLFNETWORK



@SPYWOLFOFFICIAL



@SPYWOLFNETWORK



@SPYWOLFNETWORK



Disclaimer

This report shows findings based on our limited project analysis, following good industry practice from the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, overall social media and website presence and team transparency details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report.

While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

DISCLAIMER:

By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice.

No one shall have any right to rely on the report or its contents, and SpyWolf and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (SpyWolf) owe no duty of care towards you or any other person, nor does SpyWolf make any warranty or representation to any person on the accuracy or completeness of the report.

The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and SpyWolf hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, SpyWolf hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against SpyWolf, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts, website, social media and team.

No applications were reviewed for security. No product code has been reviewed.